(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－261423
（P2000－261423A）
(43)公開日　平成12年９月22日(2000.9.22)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード（参考）
Ｈ０４Ｌ　9/06		Ｈ０４Ｌ　9/00	６１１Ｚ　５Ｊ１０４
Ｇ０９Ｃ　1/00	６１０	Ｇ０９Ｃ　1/00	６１０Ａ

審査請求　未請求　請求項の数５　ＯＬ　（全 11 頁）

(21)出願番号　特願平11－58210

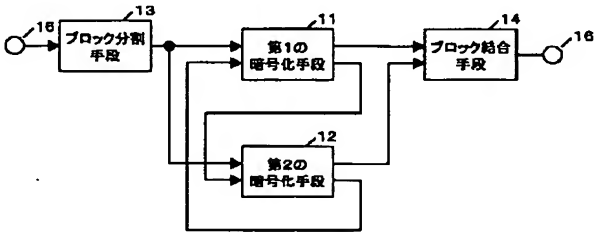
(22)出願日　平成11年３月５日(1999.3.5)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　柳澤　玲互
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100097445
弁理士　岩橋　文雄　（外２名）

Ｆターム(参考)　5J104 AA18 JA03

(54)【発明の名称】　暗号化装置

(57)【要約】
【課題】　大規模なメモリを使用することなく、暗号化の処理速度を約２倍に改善する。
【解決手段】　ブロック分割手段１３は、入力パケットをブロックに分割し、交互に第１の暗号化手段１１と第２の暗号化手段１２へ出力する。第１の暗号化手段１１は、第２の中間データを用いてブロック暗号化を行い、第１の中間データと暗号化された第１のブロックを出力する。第２の暗号化手段１２は、第１の暗号化手段１１が第１の中間データを処理する遅延だけ遅れて処理を開始し、第１の中間データを用いてブロック暗号化を行い、第２の中間データと暗号化された第２のブロックを出力する。ブロック結合手段１４は、暗号化された第１のブロックと第２のブロックとを結合し、暗号化されたパケットを出力する。



【特許請求の範囲】
【請求項１】　入力データを第１のブロックと第２のブロックとに分割して出力するブロック分割手段と、
前記第１のブロックと第２の中間データを用い前記第１のブロックを暗号化し、第１の暗号化データと第１の中間データを出力する第１の暗号化手段と、
前記第２のブロックと前記第１の中間データを用い前記第２のブロックを暗号化し、第２の暗号化データと前記第２の中間データを出力する第２の暗号化手段と、
前記第１の暗号化データと前記第２の暗号化データを結合し、前記入力データを暗号化した暗号化データを出力するブロック結合手段とを備えたことを特徴とする暗号化装置。
【請求項２】　第１の暗号化手段は、第１のブロックを暗号化し第１の中間データを出力する第３の暗号化手段と、前記第１の中間データを暗号化し前記第１の暗号化データを出力する第４の暗号化手段とからなり、
第２の暗号化手段は、第２のブロックを暗号化し第２の中間データを出力する第５の暗号化手段と、前記２の中間データを暗号化し前記第２の暗号化データを出力する第６の暗号化手段とからなることを特徴とする請求項１記載の暗号化装置。
【請求項３】　ブロック分割手段は、入力データを（ｍ＋ｎ）個（ｍ、ｎは自然数）のサブブロックに分割し、分割された先頭から奇数番目のｍ個の前記サブブロックを第１のブロックとして出力し、先頭から偶数番目のｎ個の前記サブブロックを第２のブロックとして出力し、
第１の暗号化手段は、前記第１のブロックを前記ｍ個のサブブロック毎にブロック暗号化し、
第２の暗号化手段は、前記第２のブロックを前記ｎ個のサブブロック毎にブロック暗号化することを特徴とする請求項１または２記載の暗号化装置。
【請求項４】　第１の暗号化手段は、第２の暗号化手段が出力するｊ番目（ｊ＝１、２、３、・・、ｎ）の第２の中間データを用い第１のブロックのｉ番目（ｉ＝１、２、３、・・、ｍ）のサブブロックのブロック暗号化を行い、ｉ番目の第１の中間データとｉ番目の第１の暗号化データを出力し、
第２の暗号化手段は、前記ｉ番目の第１の中間データを用い第２のブロックのｊ番目の前記サブブロックのブロック暗号化を行い、前記ｊ番目の第２の中間データとｊ番目の第２の暗号化データを出力することを特徴とする請求項３記載の暗号化装置。
【請求項５】　第１の暗号化手段は、ｉ番目の第１の中間データを遅延Ｔで、ｉ番目の第１の暗号化データを前記遅延Ｔの２倍の遅延で出力し、
第２の暗号化手段は、ｊ番目の第２の中間データを前記遅延Ｔで、ｊ番目の第２の暗号化データを前記遅延Ｔの２倍の遅延で出力し、かつ前記第１の暗号化手段より前記遅延Ｔだけ遅れて暗号化を行うことを特徴とする請求項４記載の暗号化装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ディジタルビデオレコーダー、セット・トップ・ボックス（Set Top Box）、パーソナルコンピューター等で、不正コピーを防止する際のコンテンツの暗号化等に用いられる、暗号化装置に関するものである。
【０００２】
【従来の技術】従来、暗号化装置として、特開平９－２３０７８８号公報に記載されたものが知られている。
【０００３】図６に、従来の暗号化装置のブロック図を示す。図６において、６１は第７の暗号化手段、６２は第８の暗号化手段、６３は第９の暗号化手段、６４１～６４６は暗号化回路、６５はレジスタ、６６は排他的論理和演算子、６７は暗号鍵、６８は平文入力端子、６９は暗号文出力端子である。以下、図６を用いて、従来の暗号化装置について説明する。
【０００４】暗号化回路６４１～６４６は、暗号化されていないデータ（以下、平文と呼ぶ）を暗号鍵６７に基づいて暗号化し、暗号化されたデータ（以下、暗号文と呼ぶ）を出力する。一般に、暗号の強度を増すため、暗号化回路は同じ構成のものが多数直列に接続される。図６では、Ｘ１からＸｍａ（ｍａは自然数）までのｍａ個の同じ構成の暗号化回路と、Ｙ１からＹｍｂ（ｍｂは自然数）までのｍｂ個の同じ構成の暗号化回路とを直列に接続している。図６ではこれらのうちＸ１（暗号化回路６４１）、Ｘ２（暗号化回路６４２）、Ｘｍａ（暗号化回路６４３）、Ｙ１（暗号化回路６４４）、Ｙ２（暗号化回路６４５）、Ｙｍｂ（暗号化回路６４６）の６個を例として示した。このように暗号化回路を多数接続して強度を増す例としては、米国における標準方式であるＤＥＳ（Data Encryption Standard）が知られている。
【０００５】端子６８からは、例えば６４ビットの平文が入力され、暗号化回路６４１～６４６でブロック暗号化が行われる。例えば、ＭＰＥＧ２（Moving Picture Experts Group 2）のＴＳＰ（Transport Stream Packet）（以下、単にＴＳＰと呼ぶ）を暗号化する場合、ＴＳＰは８ビット長であるので、図示していない変換回路にて８個のＴＳＰをひとまとめにして６４ビット長の平文に変換した後、端子６８から入力する。
【０００６】図６では、暗号化回路６４１～６４３で構成される第８の暗号化手段６２の出力を、一旦レジスタ６５に記憶し、次の平文が入力された時に、演算子６６でレジスタ６５と次の平文との排他的論理和をとる構成にしている。これはＣＢＣ（Cipher Block Chaining）モードと呼ばれ、暗号文の解読を困難にするための一つの手法である。
【０００７】例えばＴＳＰの場合、先頭から６４ビット毎にサブブロックに分割し、端子６８より入力する。こ

のサブブロックを先頭から順に第１サブブロック、第２サブブロック、第３サブブロックと呼ぶことにすると、まず第８の暗号化手段６２で第１サブブロックのブロック暗号化を行い、結果を第９の暗号化手段６３に出力するとともにレジスタ６５に蓄える。暗号化回路６４４～６４６で構成される第９の暗号化手段６３は、引き続き第１サブブロックのブロック暗号化を行い、暗号化された第１サブブロックを端子６９より出力する。

【０００８】次に、端子６８より入力された第２サブブロックは、レジスタ６５と演算子６６で排他的論理和がとられた後、暗号化回路６４１～６４３でブロック暗号化が行われる。この結果はレジスタ６５に蓄えられ、次の第３サブブロックのブロック暗号化に使用される。また、第９の暗号化手段６３では引き続きブロック暗号化を行い、暗号化された第２サブブロックを端子６９より出力する。

【０００９】上記した処理をＴＳＰの終わりまで繰り返し行うことで、１パケット分の暗号化を行うことができる。なお、端子６９からはサブブロックに分割された暗号文が出力されるため、図示していない逆変換回路にて、サブブロックをＴＳＰに逆変換することで、暗号化されたＴＳＰが得られる。

【００１０】ＣＢＣモードとしては、図７のような構成も知られている。図７では、レジスタ６５と暗号鍵６７との排他的論理和をとった結果を、次の平文の暗号鍵としている。図６、図７のいずれにせよ、第８の暗号化手段６２の出力と入力された平文から、次の暗号化を行い、結果を第９の暗号化手段でさらに暗号化することで、端子６９より暗号文が出力される。

【００１１】図６あるいは図７の動作を、タイミングチャートにして図８に示す。入力される平文Ｐ１０、Ｐ２０に対して、第７の暗号化手段６１の処理遅延Ｔ０だけ遅れて、暗号文Ｃ１０、Ｃ２０が出力される。ＴＳＰの場合、１パケットが１８８バイトであるから、２４のサブブロックに分割される。よって、１パケット分の処理遅延ＴＸはＴＸ＝２４×Ｔ０となる。

【００１２】第７の暗号化手段６１の処理遅延Ｔ０は、暗号化回路６４１～６４６各々の処理遅延と、全体の段数（ｍａ＋ｍｂ）で決定される。これらは共に暗号の強度に関係し、暗号の強度をある一定レベル以上に保つためには、処理遅延Ｔ０をある遅延より小さくすることができない。すなわち、１パケット分の処理遅延ＴＸをある遅延より短くすることができない。よって、高いビットレートのＴＳＰに対しては、第７の暗号化手段６１を複数用意し、それらを並列に処理することで、見かけ上の処理遅延を短くする必要がある。

【００１３】図９に、約２倍のビットレートのＴＳＰまで、処理を行う場合の構成を示す。図９において、９１は第１０の暗号化手段、９２～９５はバッファ、９６はパケット分割手段、９７はパケット結合手段である。以下、図９を用いて、約２倍のビットレートのＴＳＰを、暗号化する場合を説明する。

【００１４】第１０の暗号化手段９１は、図１０に示すように第７の暗号化手段６１と全く同じ構成を有し、第１１の暗号化手段９２と第１２の暗号化手段９３によるＣＢＣモードを備え、１パケットのブロック暗号化を行う。なお、第７の暗号化手段６１が図７のＣＢＣモードを備えるときは、同様に図１１のＣＢＣモードを備えている。

【００１５】端子６８より入力されるＴＳＰは、１パケット毎にパケット分割手段９６で分割され、１パケット毎にバッファ９２およびバッファ９３へ、交互に書き込まれる。ここで、バッファ９２，バッファ９３は、例えばＦＩＦＯ（First In FirstOut memory）である。

【００１６】バッファ９２に書き込まれたＴＳＰは、第７の暗号化手段６１で暗号化され、バッファ９４に書き込まれる。同様にバッファ９３に書き込まれたＴＳＰは、第１０の暗号化手段９１で暗号化され、バッファ９５に書き込まれる。ここで、バッファ９４，バッファ９５は、例えばＦＩＦＯである。

【００１７】この時のタイミングチャートを、図１２に示す。以下、図１２を用いて、図９の動作を説明する。

【００１８】端子６８から入力されたＴＳＰであるＰ１００、Ｐ２００、Ｐ３００、Ｐ４００は、パケット分割手段９６で分割され、Ｐ１００、Ｐ３００はバッファ９２に、Ｐ２００、Ｐ４００はバッファ９３に書き込まれる。第７の暗号化手段６１はＰ１００、Ｐ３００を順次暗号化し、結果の暗号文Ｃ１００、Ｃ３００をバッファ９４に書き込む。同様に、第１０の暗号化手段９１はＰ２００、Ｐ４００を順次暗号化し、結果の暗号文Ｃ２００、Ｃ４００をバッファ９５に書き込む。

【００１９】パケット結合手段９７は、バッファ９４、バッファ９５より交互に暗号文を読み出す。これにより、端子６８から入力されるＰ１００、Ｐ２００、Ｐ３００、Ｐ４００を暗号化した結果Ｃ１００、Ｃ２００、Ｃ３００、Ｃ４００が端子６９より順次出力される。また、この時、第７の暗号化手段６１と第１０の暗号化手段９１とが並列に動作するため、図８に比べて約２倍のビットレートのＴＳＰまで、図１２では処理している。

【００２０】

【発明が解決しようとする課題】しかしながら上記した従来の構成では、約２倍のビットレートのＴＳＰを処理するために、新たにＦＩＦＯを追加する必要があり、回路規模の増大とコストの上昇を招くという問題点を有していた。

【００２１】本発明は上記従来の問題点を解決するもので、ＦＩＦＯを追加しなくとも約２倍のビットレートのＴＳＰまで処理可能な、暗号化装置を提供することを目的とする。

【００２２】

【課題を解決するための手段】この課題を解決するために本発明は、入力データを第１のブロックと第２のブロックとに分割して出力するブロック分割手段と、前記第１のブロックと第２の中間データを用い前記第１のブロックを暗号化し、第１の暗号化データと第１の中間データを出力する第１の暗号化手段と、前記第２のブロックと前記第１の中間データを用い前記第２のブロックを暗号化し、第２の暗号化データと前記第２の中間データを出力する第２の暗号化手段と、前記第１の暗号化データと前記第２の暗号化データを結合し前記入力データを暗号化した暗号化データを出力するブロック結合手段とから構成されている。

【００２３】

【発明の実施の形態】本発明は、ブロック分割手段で、入力データを第１のブロックと第２のブロックとに分割する。第１の暗号化手段は、第２の中間データを用い、第１のブロックを暗号化し、第１の中間データと第１のブロックを暗号化した結果である第１の暗号化データを出力する。第２の暗号化手段は、第１の中間データを用い、第２のブロックを暗号化し、第２の中間データと第２のブロックを暗号化した結果である第２の暗号化データを出力する。ブロック結合手段は、第１の暗号化データと第２の暗号化データを結合し、入力データを暗号化した暗号化データを出力する。

【００２４】以下、本発明の実施の形態について、図面を用いて説明する。

【００２５】（実施の形態１）図１は、本発明の実施の形態１による暗号化装置のブロック図を示すものである。図１において、１１は第１の暗号化手段、１２は第２の暗号化手段、１３はブロック分割手段、１４はブロック結合手段、１５は平文入力端子、１６は暗号文出力端子である。以下、図１を参照しながら、本実施の形態の暗号化装置について説明する。

【００２６】ブロック分割手段１３は、端子１５より入力される平文を、２つのブロックに分割する。例えば端子１５よりＴＳＰが入力される場合、まず先頭から６４ビット毎のサブブロックに分割し、次に先頭から１番目、３番目、５番目、・・・、すなわち、奇数番目のサブブロックを第１のブロックとして、第１の暗号化手段１１に出力する。同様に先頭から偶数番目のサブブロックを、第２のブロックとして、第２の暗号化手段１２に出力する。このような動作を行うブロック分割手段１３には、例えばデマルチプレクサが用いられる。

【００２７】第１の暗号化手段１１と第２の暗号化手段１２の構成例を、図２に示す。図２において、２１は第３の暗号化手段、２２は第４の暗号化手段、２３は第５の暗号化手段、２４は第６の暗号化手段、２５１～２５６および２６１～２６６は暗号化回路、２７、２８はレジスタ、２９、２１０は排他的論理和演算子、２１１、２１２は暗号鍵である。以下、図２を参照しながら、第１の暗号化手段１１と第２の暗号化手段１２の暗号化の動作について説明する。

【００２８】第１の暗号化手段１１は、第１のブロックの暗号化を、暗号鍵２１１を用いて行う。まず１番目のサブブロックが入力されると、暗号化回路２５１～２５３でブロック暗号化を行い、１番目の第１の中間データを出力する。従来の技術の項で説明したように、暗号の強度を増すため、同様の構成の暗号化回路２５１～２５３をｍａ段直列に接続している。

【００２９】第１の暗号化手段１１，第２の暗号化手段１２は、共にＣＢＣモードを有しており、入力されるサブブロックとレジスタ２７、２８との排他的論理和を演算子２９、２１０で行う構成をとっている。ＣＢＣモードとしては、図３に示すように、レジスタ２７、２８と暗号鍵２１１、２１２との排他的論理和をとる構成としてもよい。

【００３０】１番目の第１の中間データは、引き続き暗号化回路２５４～２５６でブロック暗号化され、暗号化された１番目のサブブロックとして出力されるとともに、第２の暗号化手段１２のレジスタ２８に一旦蓄えられる。暗号化回路２５４～２５６はｍｂ段で構成され、暗号化回路２５１～２５３と合わせて、全体でｍａ＋ｍｂ＝ｍ段（ｍは自然数）の暗号化回路を構成している。

【００３１】第２のブロックの暗号化は第２の暗号化手段１２で行われるため、２番目のサブブロックが入力されると、まずレジスタ２８に蓄えられている１番目の第１の中間データと、２番目のサブブロックとの排他的論理和が、演算子２１０でとられる。次に、ｎａ段（ｎａは自然数）の暗号化回路２６１～２６３で、暗号鍵２１２を用いたブロック暗号化が行われ、１番目の第２の中間データが出力される。

【００３２】１番目の第２の中間データは、引き続きｎｂ段（ｎｂは自然数）の暗号化回路２６４～２６６でブロック暗号化され、暗号化された２番目のサブブロックとして出力されるとともに、第１の暗号化手段１１のレジスタ２７に一旦蓄えられる。暗号化回路２５４～２５６と、暗号化回路２５１～２５３とを合わせて、全体でｎａ＋ｎｂ＝ｎ段（ｎは自然数）の暗号化回路を構成している。

【００３３】次に３番目のサブブロックが入力されると、レジスタ２７に蓄えられた１番目の第２の中間データとの排他的論理和が演算子２９でとられ、暗号化回路２５１～２５３でブロック暗号化され、２番目の第１の中間データが出力される。これを一旦レジスタ２８に蓄えるとともに、暗号化回路２５４～２５６でブロック暗号化し、暗号化された３番目のサブブロックとして出力する。

【００３４】同様の操作を繰り返すことで、暗号化されたサブブロックが次々に出力される。この時のタイミングチャートを図４に示す。図４では、第３の暗号化手段

の処理遅延をＴ３、第４の暗号化手段の処理遅延をＴ４、第５の暗号化手段の処理遅延をＴ５、第６の暗号化手段の処理遅延をＴ６、第１の暗号化手段の処理遅延をＴ１（＝Ｔ３＋Ｔ４）、第２の暗号化手段の処理遅延をＴ２（＝Ｔ５＋Ｔ６）とし、Ｔ３＝Ｔ４＝Ｔ５＝Ｔ６の場合を示した。なお、この時、ｍａ＝ｍｂ＝ｎａ＝ｎｂ、すなわちｍ＝ｎである。

【００３５】第３の暗号化手段の処理遅延Ｔ３後、１番目の第１の中間データが出力され、さらに第４の暗号化手段の処理遅延Ｔ４の後、暗号化された１番目のサブブロックが出力される。暗号化手段１２は、第３の暗号化手段の処理遅延Ｔ３だけ遅れて処理を開始する。すなわち、１番目の第１の中間データが出力されてから処理を開始する。第５の暗号化手段の処理遅延Ｔ５の後、１番目の第２の中間データが出力され、さらに第６の暗号化手段の処理遅延Ｔ６の後、暗号化された２番目のサブブロックが出力される。

【００３６】以下同様に、第１の暗号化手段１１と第２の暗号化手段１２とがサブブロック毎に交互に動作し、端子１５より入力される平文の暗号化を行う。ブロック結合手段１４は、第１の暗号化手段１１と第２の暗号化手段１２とが出力するサブブロック毎の暗号文を交互に出力することで、端子１５より入力される平文の暗号文を、端子１６より出力する。このような動作を行うブロック結合手段１４には、例えばマルチプレクサが用いられる。

【００３７】図５に、平文としてＴＳＰを用いた場合のタイミングチャートを示す。図５において、Ｐ１～４は入力されるＴＳＰ、Ｃ１～４が暗号化されたＴＳＰである。暗号化されたＴＳＰであるＣ１～４は、入力ＴＳＰであるＰ１～４より暗号化の処理遅延だけ遅れて出力される。この処理遅延は図４、図５に示すように、Ｔ３＋Ｔ５になる。

【００３８】また、ＴＳＰの場合、１パケットが１８８バイトであるから、１パケットは２４のサブブロックに分割される。よって、第１の暗号化手段１１の処理遅延ＴＡは１２×Ｔ１、第２の暗号化手段１２の処理遅延ＴＢは１２×Ｔ２となる。この処理遅延ＴＡ、ＴＢは、Ｔ１＝Ｔ２、Ｔ３＝Ｔ４＝Ｔ５＝Ｔ６の時最小となり、第１の暗号化手段１１単独で暗号化した時の処理遅延２４×Ｔ１、あるいは第２の暗号化手段１２単独で暗号化した時の処理遅延２４×Ｔ２の、約２倍のビットレートのＴＳＰまで処理することが可能になる。

【００３９】なお、本実施例では、平文がＴＳＰの場合を例にとって説明したが、どのような平文に対しても、最大で約２倍の処理速度で暗号化を行うことができる。また、処理速度が最小となるＴ１＝Ｔ２、Ｔ３＝Ｔ４＝Ｔ５＝Ｔ６の場合を説明したが、この条件に当てはまらない場合でも、処理速度を改善することができ、ビットレートの高い平文に対して効果がある。

【００４０】

【発明の効果】以上のように本発明によれば、入力データを第１のブロックと第２のブロックとに分割して出力するブロック分割手段と、第２の中間データを用い第１のブロックを暗号化し第１の暗号化データと第１の中間データを出力する第１の暗号化手段と、第１の中間データを用い第２のブロックを暗号化し第２の暗号化データと第２の中間データを出力する第２の暗号化手段と、第１の暗号化データと第２の暗号化データを結合し暗号化データを出力するブロック結合手段とを設けることにより、大容量のメモリを使用しなくとも容易に暗号化の処理速度が改善でき、その実用的効果は大きい。

【図面の簡単な説明】

【図１】本発明の実施の形態１における暗号化装置の構成を示すブロック図

【図２】同実施の形態１における第１の暗号化手段および第２の暗号化手段の具体的な構成例を示すブロック図

【図３】同実施の形態１における別のＣＢＣモードの構成例を示すブロック図

【図４】同実施の形態１における第１の暗号化手段および第２の暗号化手段の動作を説明する信号波形図

【図５】同実施の形態１における暗号化装置の動作を説明する信号波形図

【図６】従来の暗号化装置の構成を示すブロック図

【図７】従来の暗号化装置における別のＣＢＣモードでの構成例を示すブロック図

【図８】従来の暗号化装置の動作を説明する信号波形図

【図９】従来の暗号化装置を約２倍の処理速度で動作させる場合の構成例を示すブロック図

【図１０】従来の暗号化装置における第１０の暗号化手段の具体的な構成例を示すブロック図

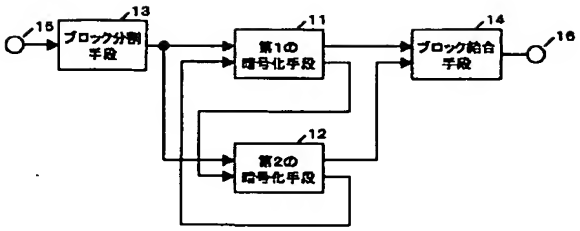
【図１１】従来の暗号化装置における第１０の暗号化手段の別のＣＢＣモードでの具体的な構成例を示すブロック図

【図１２】従来の暗号化装置を約２倍の処理速度で動作させる場合の動作を説明する信号波形図

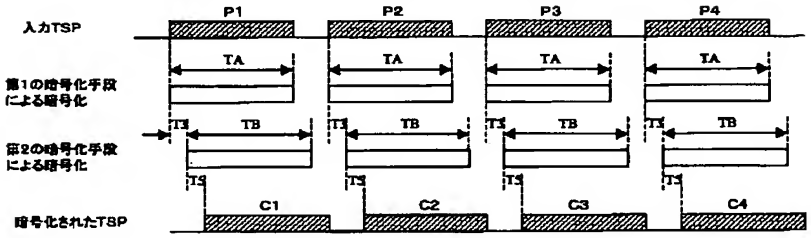
【符号の説明】

１１　第１の暗号化手段
１２　第２の暗号化手段
１３　ブロック分割手段
１４　ブロック結合手段

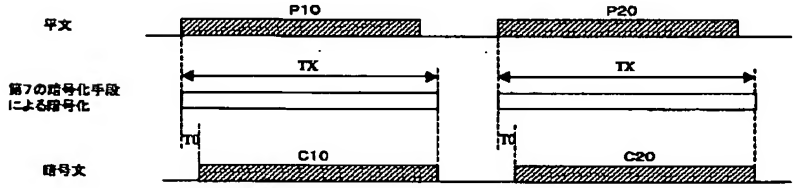
【図１】


15
13
ブロック分割手段
11
第1の暗号化手段
12
第2の暗号化手段
14
ブロック結合手段
16

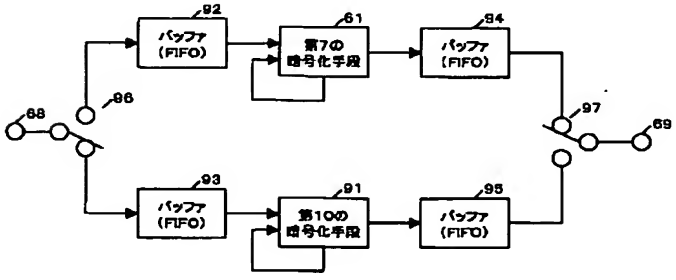
【図５】


入力TSP
P1
P2
P3
P4
第1の暗号化手段による暗号化
TA
第2の暗号化手段による暗号化
TB
暗号化されたTSP
C1
C2
C3
C4

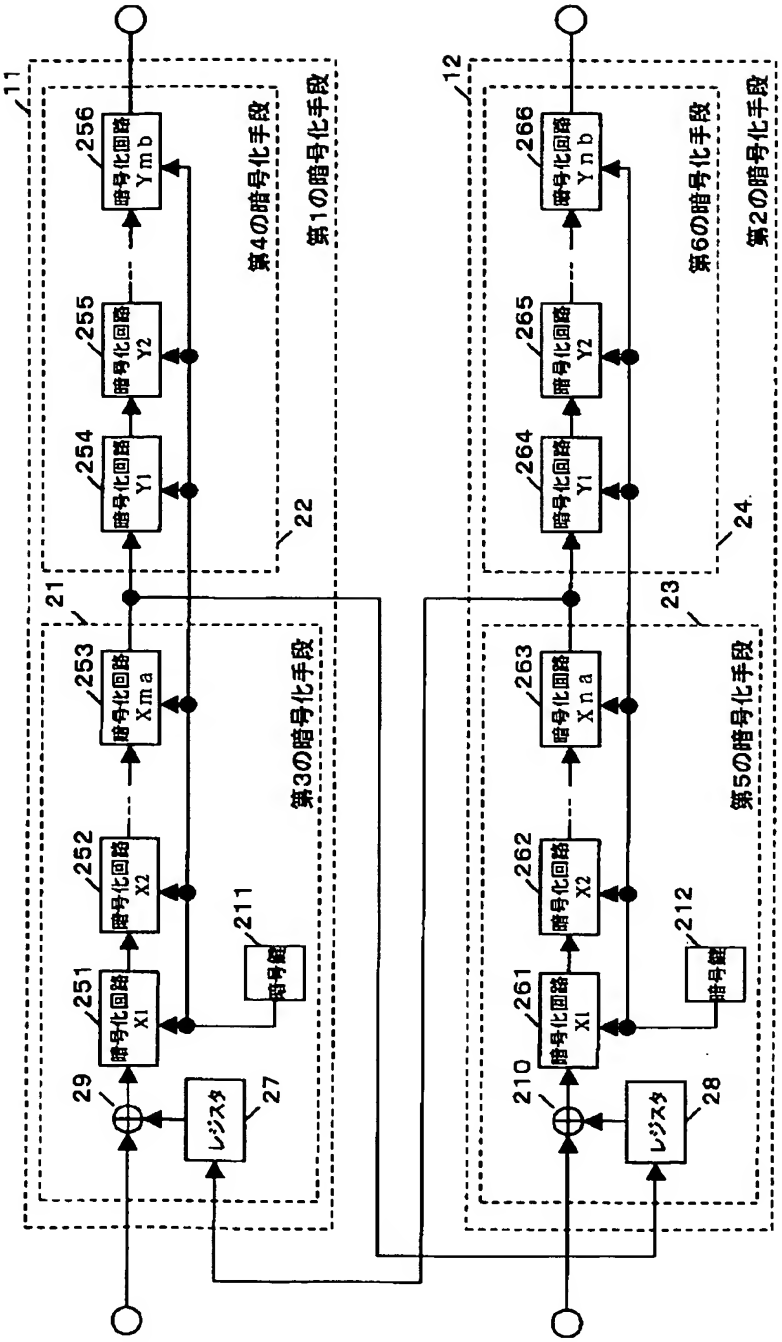
【図８】


平文
P10
P20
第7の暗号化手段による暗号化
TX
暗号文
C10
C20

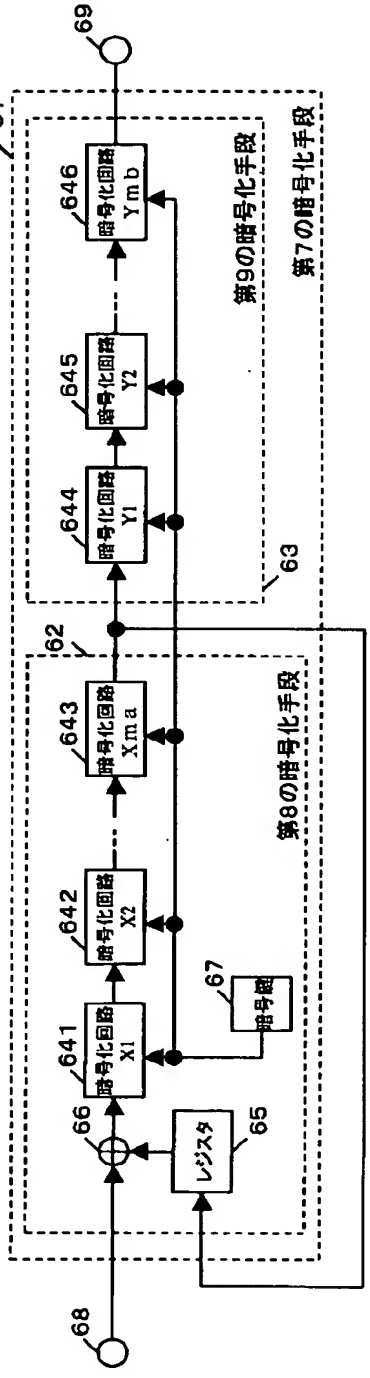
【図９】


92
バッファ(FIFO)
61
第7の暗号化手段
94
バッファ(FIFO)
68
96
97
69
93
バッファ(FIFO)
91
第10の暗号化手段
95
バッファ(FIFO)

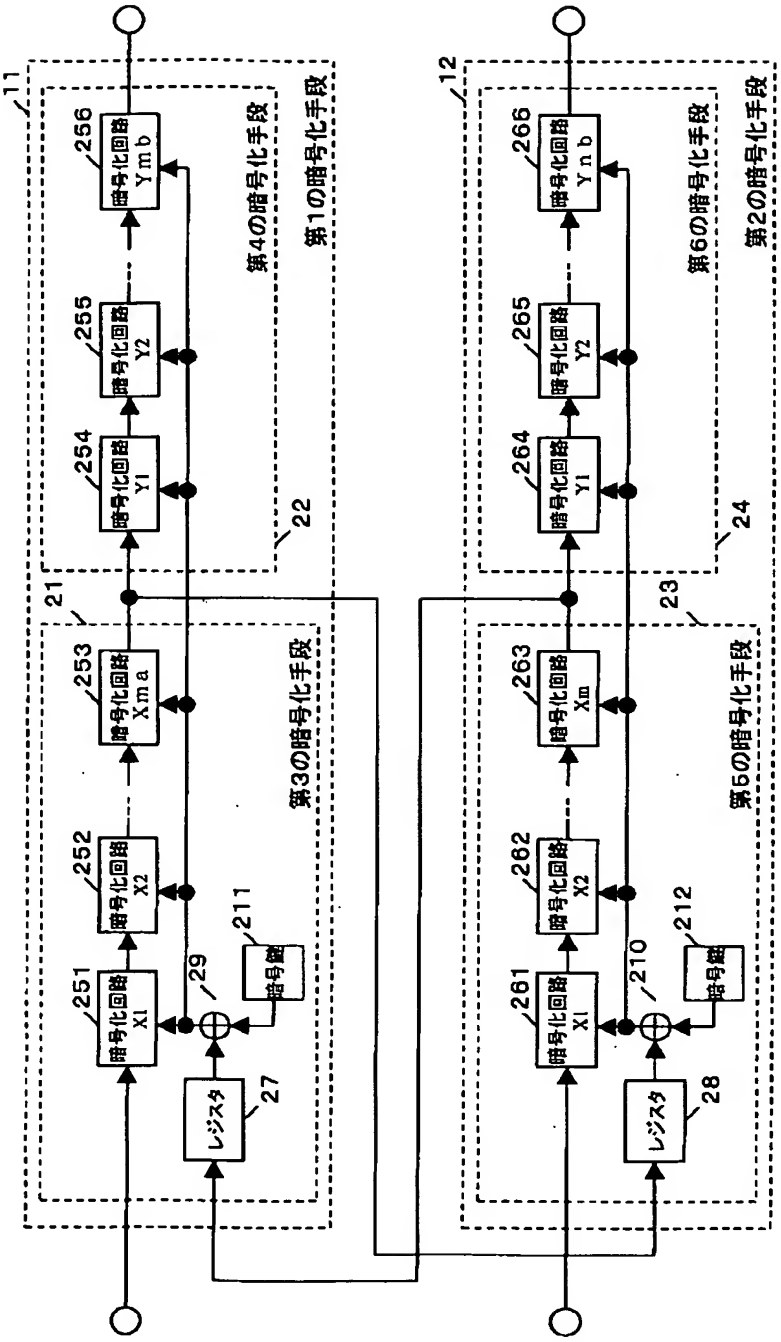
【図２】


11
第1の暗号化手段
21
第3の暗号化手段
暗号化回路 X1
暗号化回路 X2
暗号化回路 Xma
暗号鍵
211
レジスタ
27
29
22
第4の暗号化手段
暗号化回路 Y1
暗号化回路 Y2
暗号化回路 Ymb
254
255
256
12
第2の暗号化手段
23
第5の暗号化手段
暗号化回路 X1
暗号化回路 X2
暗号化回路 Xna
暗号鍵
212
レジスタ
28
210
24
第6の暗号化手段
暗号化回路 Y1
暗号化回路 Y2
暗号化回路 Ynb
264
265
266

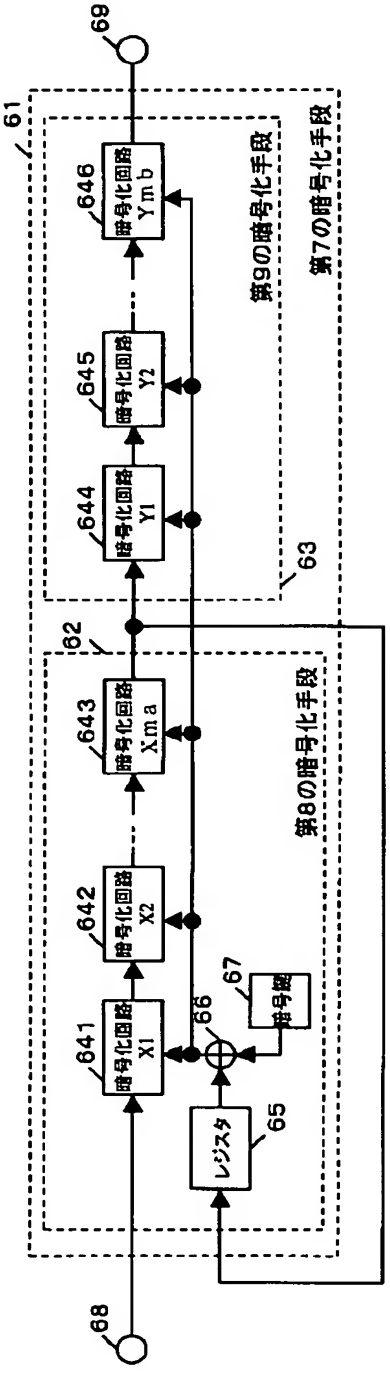
【図６】


61
第7の暗号化手段
62
第8の暗号化手段
暗号化回路 X1
暗号化回路 X2
暗号化回路 Xma
暗号鍵
67
レジスタ
65
66
63
第9の暗号化手段
暗号化回路 Y1
暗号化回路 Y2
暗号化回路 Ymb
644
645
646
68
69

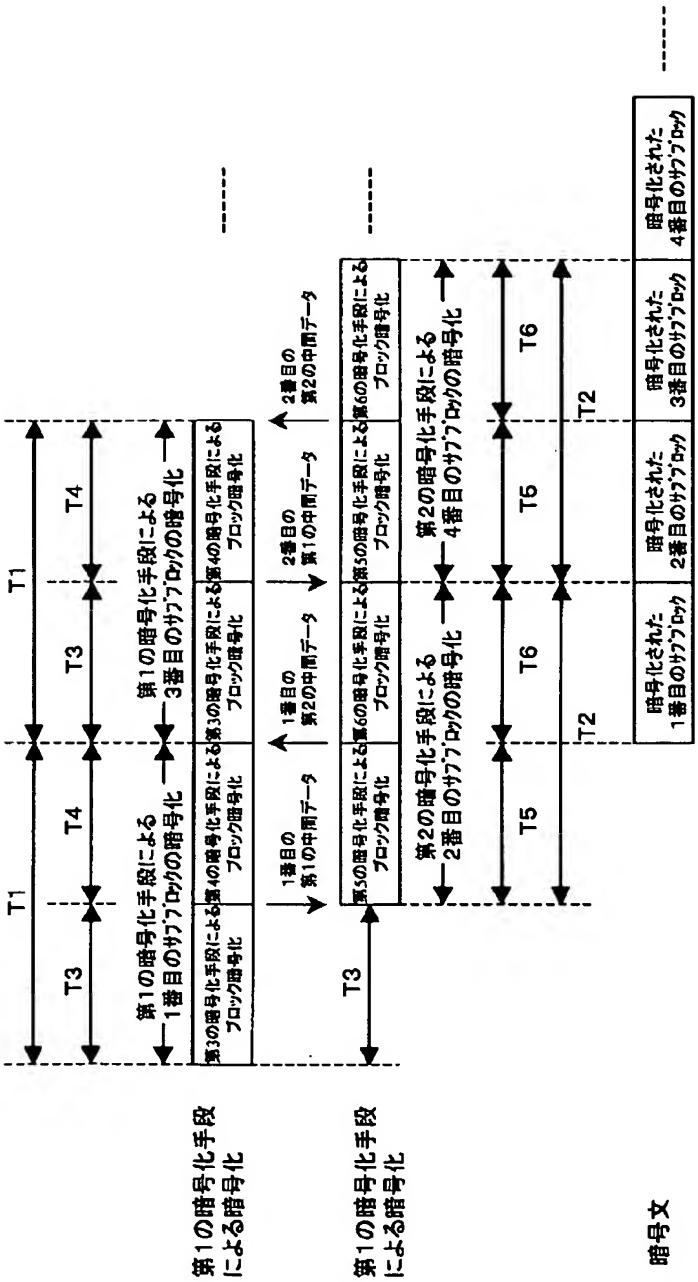
【図３】


11
第1の暗号化手段
21
第3の暗号化手段
251
暗号化回路 X1
252
暗号化回路 X2
253
暗号化回路 Xma
22
第4の暗号化手段
254
暗号化回路 Y1
255
暗号化回路 Y2
256
暗号化回路 Ymb
29
211
暗号鍵
27
レジスタ
12
第2の暗号化手段
23
第5の暗号化手段
261
暗号化回路 X1
262
暗号化回路 X2
263
暗号化回路 Xm
24
第6の暗号化手段
264
暗号化回路 Y1
265
暗号化回路 Y2
266
暗号化回路 Ynb
210
212
暗号鍵
28
レジスタ

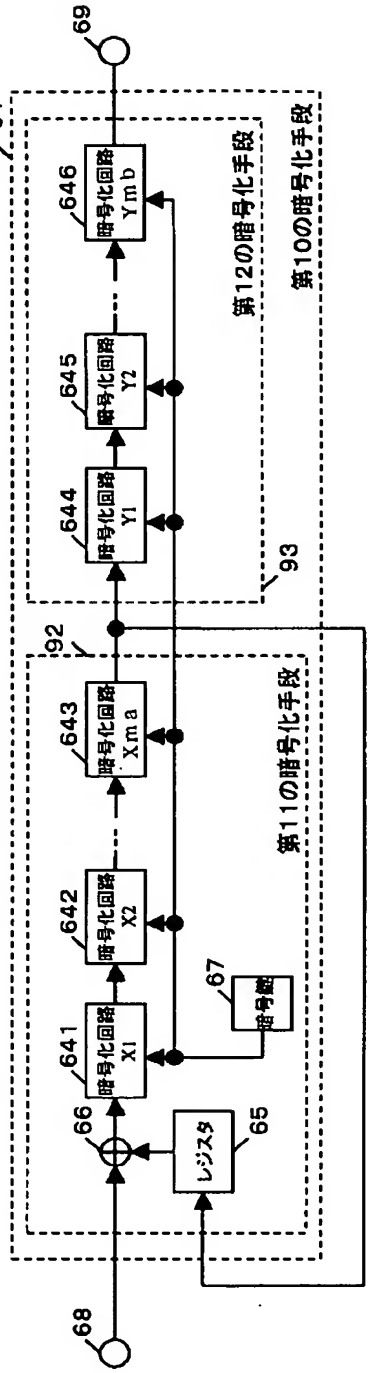
【図７】


69
61
第7の暗号化手段
62
第8の暗号化手段
641
暗号化回路 X1
642
暗号化回路 X2
643
暗号化回路 Xma
63
第9の暗号化手段
644
暗号化回路 Y1
645
暗号化回路 Y2
646
暗号化回路 Ymb
66
67
暗号鍵
65
レジスタ
68

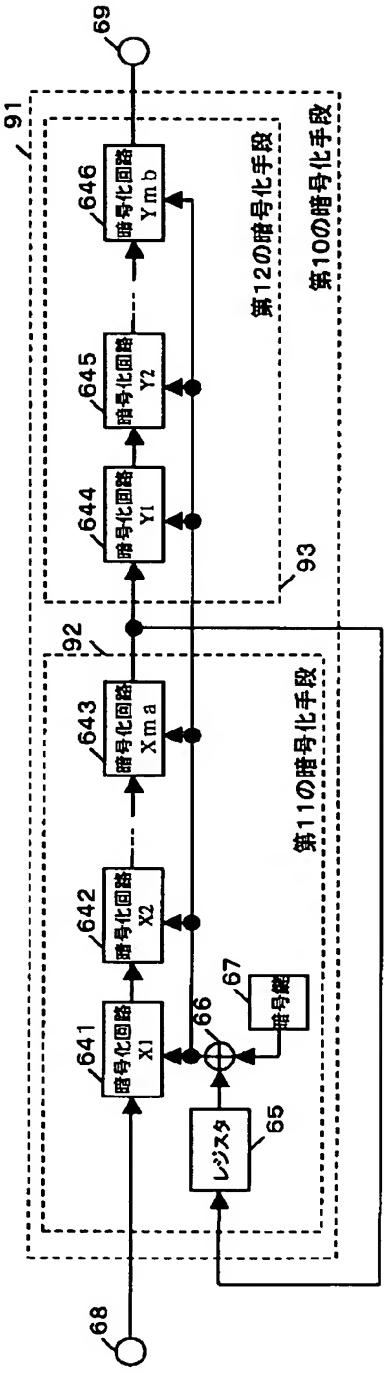
【図４】


第1の暗号化手段による暗号化
第1の暗号化手段による
1番目のサブブロックの暗号化
第1の暗号化手段による
3番目のサブブロックの暗号化
第1の暗号化手段による暗号化
第2の暗号化手段による
2番目のサブブロックの暗号化
第2の暗号化手段による
4番目のサブブロックの暗号化
T1
T2
T3
T4
T5
T6
1番目の第1の中間データ
1番目の第2の中間データ
2番目の第1の中間データ
2番目の第2の中間データ
暗号化されたサブブロック
暗号文

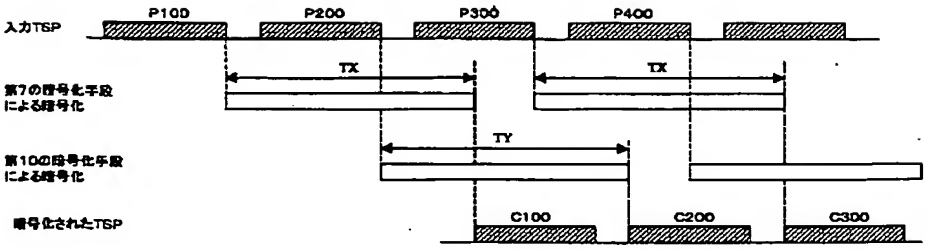
【図１０】


69
91
646
暗号化回路 Ymb
645
暗号化回路 Y2
644
暗号化回路 Y1
643
暗号化回路 Xma
642
暗号化回路 X2
641
暗号化回路 X1
92
93
67
暗号鍵
66
レジスタ
65
68
第12の暗号化手段
第10の暗号化手段
第11の暗号化手段

【図１１】


69
91
第10の暗号化手段
第12の暗号化手段
646
暗号化回路
Ymb
645
暗号化回路
Y2
644
暗号化回路
Y1
93
92
第11の暗号化手段
643
暗号化回路
Xma
642
暗号化回路
X2
641
暗号化回路
X1
67
暗号鍵
66
レジスタ
65
68

【図１２】


入力TSP
P100
P200
P300
P400
TX
TX
第7の暗号化手段
による暗号化
TY
第10の暗号化手段
による暗号化
暗号化されたTSP
C100
C200
C300